

CLAIMS

What is claimed is:

1. A system for facilitating digital signing of electronic messages comprising:
5 a browser;
a signing module; and
a signing interface, the signing interface adapted to be invoked by a Web application
transmitted to the browser from a remote location, and to:
forward data to be signed to the signing module,
10 receive a digital signature for the data to be signed from the signing module, and
forward the digital signature to a remote location specified by the Web application.
2. The system of claim 1, wherein the signing interface comprises a signing interface
library having an API and the Web application is an applet referenced in a Web page
15 transmitted to the browser from a Web server.
3. The system of claim 2, wherein the applet is adapted to retrieve the data to be signed
from a remote location and to forward the data to be signed to the signing interface.
- 20 4. The system of claim 2, wherein the applet is digitally signed.
5. The system of claim 1, wherein the signing interface comprises a signing plug-in and
the Web application is a Web page comprising a tag adapted to launch the signing plug-in.
- 25 6. The system of claim 5, wherein the tag is an <EMBED> tag.
7. The system of claim 5, wherein the tag is an <OBJECT> tag.
8. The system of claim 1, wherein the data to be signed is retrieved from a remote
30 location specified by the Web application.
9. The system of claim 1, wherein the data to be signed is included in the Web
application.
- 35 10. The system of claim 1, wherein the signing module digitally signs the data to be
signed with an identity key.

11. The system of claim 1, wherein the signing module is a smart card subsystem.
12. The system of claim 1, wherein the digitally signed data includes card and signature security data.
- 5 13. The system of claim 1, wherein the signing interface is obtained from a trusted entity.
14. The system of claim 13, wherein the signing interface is digitally signed by the trusted entity.
- 10 15. The system of claim 14, wherein the trusted entity is an issuing participant.
16. The system of claim 1, wherein the signing interface comprises a user interface.
17. The system of claim 16, wherein the user interface displays the data to be signed to a
15 user and obtains the user's approval to sign the data.
18. The system of claim 16, wherein the user interface offers a user the opportunity to store the data to be signed.
- 20 19. The system of claim 16, wherein the user interface offers a user the opportunity to view the data to be signed in a software application.
20. The system of claim 19, wherein the software application is a spreadsheet.
- 25 21. A method for facilitating digital signing of electronic messages comprising:
a browser,
a signing module,
and a signing interface, the signing interface adapted to be invoked by a Web
application transmitted to the browser from a remote location, the method comprising:
30 invoking the signing interface;
forwarding by the signing interface the data to be signed to the signing module;
receiving at the signing interface a digital signature for data to be signed from the
signing module; and
forwarding the digital signature to a remote location specified by the Web
35 application.

22. The method of claim 21, wherein the signing interface comprises a signing interface library having an API and the Web application is an applet referenced in a Web page transmitted to the browser from a Web server.
23. The method of claim 22, wherein the applet is adapted to retrieve the data to be signed from a remote location and to forward the data to be signed to the signing interface.
24. The method of claim 22, wherein the applet is digitally signed.
25. The method of claim 21, wherein the signing interface comprises a signing plug-in and the Web application is a Web page comprising a tag adapted to launch the signing plug-in.
26. The method of claim 25, wherein the tag is an <EMBED> tag.
27. The method of claim 25, wherein the tag is an <OBJECT> tag.
28. The method of claim 21, wherein the data to be signed is retrieved from a remote location specified by the Web application.
29. The method of claim 21, wherein the data to be signed is included in the Web application.
30. The method of claim 21, wherein the signing module digitally signs the data to be signed with an identity key.
31. The method of claim 21, wherein the signing module is a smart card subsystem.
32. The method of claim 21, wherein the digitally signed data includes card and signature security data.
33. The method of claim 21, wherein the signing interface is obtained from a trusted entity.
34. The method of claim 33, wherein the signing interface is digitally signed by the trusted entity.

35. The method of claim 34, wherein the trusted entity is an issuing participant.
36. The method of claim 21, wherein the signing interface comprises a user interface.
37. The method of claim 36, wherein the user interface displays the data to be signed to a
5 user and obtains the user's approval to sign the data.
38. The method of claim 36, wherein the user interface offers a user the opportunity to store the data to be signed.
- 10 39. The method of claim 36, wherein the user interface offers a user the opportunity to view the data to be signed in a software application.
40. The method of claim 39, wherein the software application is a spreadsheet.
- 15 41. A system for facilitating signing by a first customer comprising:
a browser;
a signing module;
a signing interface, the signing interface being adapted to facilitate access to system
services provided via a four-corner model comprising a root entity, a first participant, a
20 second participant, the first customer, and a second customer, the second customer
maintaining a second-customer computer system;
means for downloading a Web application from the second-customer computer
system to the browser;
means for invoking the signing interface;
25 means for determining whether to request a system service;
means for creating a service request for the system service;
means for transmitting the service request;
means for receiving a response to the service request;
means for forwarding the data to be signed to the signing module;
30 means for receiving a digital signature for the data to be signed from the signing
module; and
means for forwarding the digital signature to a remote location specified by the Web
application.
- 35 42. The system of claim 41, further comprising means for presenting to the first customer an option to request a system service.

43. The system of claim 42, wherein the system service is a warranty.

44. The system of claim 43, wherein the response to the service request comprises a warranty and wherein the warranty is forwarded with the digital signature to the remote location specified by the Web application.

5

45. A method for accessing system services provided via a four-corner model, the four corner model comprising:

a root entity,

a first participant,

10

a second participant,

a first customer, the first customer being a customer of the first participant, and maintaining a first-customer computer system, the first-customer computer system comprising:

a browser,

15

a signing module,

and a signing interface,

a second customer, the second customer being a customer of the second participant, the second customer maintaining a second-customer computer system, the second-customer computer system comprising a Web server adapted to serve Web pages to the first-customer computer system's browser, the method comprising:

20

invoking the signing interface;

retrieving data to be signed from a remote location;

determining whether to request a system service;

creating a service request for the system service;

25

transmitting the service request;

receiving a response to the service request;

forwarding the data to be signed to the signing module;

receiving a digital signature for the data to be signed from the signing module; and

forwarding the digital signature to a remote location specified by the Web application.

30

44. The method of claim 43, further comprising: presenting to the first customer an option to request a system service.

45. The method of claim 44, wherein the system service is a warranty.

35

46. The method of claim 45, wherein the response to the service request comprises a warranty and wherein the warranty is forwarded with the digital signature to the remote location specified by the Web application.

5

10

15

20

25

30

35